Revista CIDOB d'Afers Internacionals
n.111, p. 127-151
ISSN:1133-6595
E-ISSN:2013-035X
www.cidob.org
Fecha de recepción: 15.06.15
Fecha de aceptación: 01.10.15

Límites del derecho europeo de protección de datos en el control de fronteras de la UE

The limits of European data protection law in EU border control

Cristina Blasi Casagran

Investigadora postdoctoral, Universitat Autònoma de Barcelona; especialista en la protección de datos en el ámbito del ELSJ. *Cristina.blasi@uab.cat*

Resumen: En los años ochenta del siglo pasado la UE empezó a recoger datos de personas que llegaban de terceros países a territorio europeo para controlar los flujos migratorios. Sin embargo, los atentados terroristas del 11-S de 2001 propiciaron una extensión progresiva del uso de tal información, originalmente solo prevista para controlar la inmigración, para fines policiales. Sistemas de información tales como SIS, VIS, CIS y Eurodac han ido reformando sus respectivas legislaciones para permitir el acceso a las autoridades policiales de los estados miembros y a Europol. Este artículo analiza el posible conflicto que se deriva de estas prácticas con el derecho fundamental de protección de datos en la UE. Se examinan, en primer lugar, las normas europeas generales y sectoriales de protección de datos aplicables para el tratamiento de la información recogida por el SIS, el VIS, el CIS y Eurodac; posteriormente, se valora si el uso de estos sistemas de información en investigaciones policiales podría vulnerar los principios de necesidad y limitación de finalidad.

Palabras clave: UE, control fronterizo, sistemas de información, protección de datos

Abstract: *In the 1980s, the EU began collecting the personal data of people arriving from third countries in order to control migratory flows within the EU. However, since the 9/11 attacks function creep has led to this information, which was originally collected for EU border management, being used by police authorities. Information systems such as SIS, VIS, CIS and Eurodac have been amending their own regulations to permit access by police authorities from the member states and Europol. This paper analyses the potential conflict arising from these practises and the fundamental right to data protection in the EU. First, general and sectoral data protection rules applicable to the data processed by SIS, VIS, CIS and Eurodac will be examined. After that, this study will assess whether allowing law enforcement authorities to access such EU information systems could violate the EU principles of necessity and purpose limitation.*

Key words: *EU, border control, information systems, data protection*

El presente trabajo se inscribe en el marco del proyecto «MAGELS» (El reto del nuevo mapa de las Agencias del Espacio de Libertad, Seguridad y Justicia de la UE), ref. DER2012-36009, financiado por el Ministerio de Economía y Competitividad.

Tal y como señalan Hijmans y Scirocco (2009: 1.491), la información se usa cuando existe. En este sentido, la Unión Europea (UE) ha ido incrementando gradualmente el número de sistemas de información y bases de datos accesibles para los entes policiales; en concreto, ha reformado diversos actos legislativos que regulan la recogida de datos personales para usos comerciales y de control transfronterizo, con el fin de permitir a las autoridades policiales acceder a los mismos. Como regla general, cuando los datos personales se recogen para un propósito concreto pero posteriormente son tratados para fines distintos al original, se puede estar vulnerando el llamado «principio de limitación de finalidad» de la UE. Este principio es uno de los principios generales para garantizar el derecho a la protección de datos personales y se encuentra recogido en el artículo 5(b) del Convenio 108 del Consejo de Europa (Consejo de Europa, 1981), el artículo 6(1)(b) de la Directiva 95/46/CE (Comunidades Europeas, 1995: 31-50) y el artículo 3 de la Decisión Marco del Consejo 2008/977/JAI (Consejo de la UE, 2008a: 60-71). Este artículo examina si los sistemas a través de los cuales la UE ha ido ampliando de manera gradual el uso de información personal para finalidades policiales pueden estar vulnerando los principios de necesidad y limitación de finalidad como parte del derecho de protección de datos de la UE.

La desviación del uso de los sistemas SIS, VIS, CIS y Eurodac

La Comisión Europea publicó una comunicación en noviembre de 2010 mediante la cual se proponía un nuevo marco para la protección de datos en la UE (Comisión Europea, 2010a). La comunicación identificaba 20 instrumentos diferentes vinculados al Espacio de Libertad, Seguridad y Justicia (ELSJ) encargados de recoger y tratar datos personales a nivel europeo. La lista incluía los Sistemas de Información de Schengen (SIS y SIS II), el Sistema de Información de Visados (VIS) y la base de datos europea de solicitantes de asilo (Eurodac). Todos ellos fueron originalmente creados para fines de control fronterizo, pero actualmente los datos que recogen pueden ser tratados para fines policiales[1]. Este cambio de finalidad fue consecuencia de los atentados del 11-S (Baldaccini, 2008: 39), ya que

1. En un futuro las autoridades policiales podrían tener acceso a otros sistemas de información, como el Sistema Entrada-Salida o el Programa de Viajeros Registrados, pero como aún no es así, estos no se examinarán en este artículo.

antes del 2001 existían muy pocos sistemas europeos para el intercambio de datos de inmigrantes accesibles a las autoridades policiales[2]. Tal y como se puede ver a continuación, la desviación en su uso aumentó de manera significativa a partir del año 2005, momento en que se empieza a observar una extensión del uso de estos sistemas para finalidades policiales.

Por lo que respecta al Sistema de Información de Schengen (SIS), su origen se sitúa en el año 1985 con la adopción del Acuerdo Schengen. Este acuerdo constituyó un hito para la política europea contra el terrorismo. Su objetivo era controlar las fronteras externas de los estados miembros y, concretamente, a los nacionales de terceros estados que entraban en territorio europeo. Solo cinco estados miembros firmaron inicialmente el acuerdo: Bélgica, Francia, Países Bajos, Luxemburgo y Alemania. Estos países implementaron el acuerdo mediante el Convenio de Aplicación del Acuerdo Schengen (CAAS) de 1990 y, a partir de ese momento, pasaron a formar parte del espacio Schengen, mediante el cual se abolieron los controles internos y se creó una frontera externa común. El CAAS incluyó un capítulo sobre el SIS, un sistema compuesto por secciones nacionales de cada Estado miembro que permitía transferir de una manera rápida y efectiva toda la información sobre controles de fronteras y desplazamiento de personas.

La Unión Europea ha ido incrementando gradualmente el número de sistemas de información y bases de datos accesibles para los entes policiales.

A través del SIS –operativo desde 1995– los estados miembros pueden mandar una alerta de personas que estén en busca y captura, o vinculadas a investigaciones policiales o a procedimientos penales, o también a las que se les haya denegado el acceso al espacio Schengen. Así mismo, se puede informar de vehículos, armas de fuego, documentos de identidad y cheques bancarios desaparecidos o robados (artículos 95-100 del CAAS). Las búsquedas por vía del SIS pueden emitir una respuesta positiva o *hit*, que especifica la acción a seguir contra personas a las que se les veta la entrada al espacio Schengen (Hayes y Vermeulen, 2012: 31). Aunque el CAAS ya introducía la posibilidad de que las autoridades policiales accedieran a los datos recogidos por el sistema, no fue hasta más tarde que la UE adoptó dos medidas legislativas nuevas que otorgaban competencia a los entes policiales: el Reglamento del Consejo 871/2004 (Consejo de la UE, 2004b: 29-31) y la Decisión del Consejo 2005/211/JAI (Consejo de la UE, 2005: 44-48).

2. Por ejemplo, la Decisión del Consejo 2000/261/JAI de 27 de marzo 2000, DO L 81, 01.04.2000, p. 1-3.

Actualmente hay más de 41.000 personas incluidas en el SIS, y el sistema emite más de 1.000 *hits* mensuales (Statewatch, 2014). El número de datos entrantes en el sistema ha ido en aumento año tras año (Consejo de la UE, 2012a) y, por ello, la Decisión del Consejo y el Reglamento del Consejo necesitaron desarrollar una segunda generación del SIS –el SIS II– que incorporara los últimos avances tecnológicos en el campo de la información (Hayes, 2004: 17). La Decisión SIS II (Consejo de la UE, 2013a: 11) persigue asegurar un alto nivel de seguridad dentro del ELSJ, mejorando las condiciones y procedimientos de alerta con respecto a los nacionales de terceros estados. Al mismo tiempo, permite intercambiar información suplementaria con el objetivo de rechazar la entrada a individuos concretos en territorio de los estados miembros. El SIS II también introduce la posibilidad de recoger datos biométricos, como huellas dactilares o fotografías, de personas con una orden de busca y captura, personas desaparecidas, personas con un procedimiento judicial abierto (por ejemplo, testigos) o bien que están sometidas a vigilancia discreta. Así mismo, tiene capacidad para 100 millones de alertas y se compone de tres subsistemas: a) un sistema central (SIS II central); b) un sistema nacional (N.SIS II) en cada Estado miembro, y c) una infraestructura para las comunicaciones en el SIS II central y los N.SIS II, mediante la oficina Sirene (cada Estado miembro tiene una oficina Sirene). Si se recibe una alerta entonces se mandará información suplementaria mediante este canal.

El Sistema de Información de Visados (VIS), por su parte, se creó en 2004 mediante la Decisión del Consejo 2004/512/CE (Decisión VIS) (Consejo de la UE, 2004a: 5-7). Su propósito era reforzar la política de inmigración de la UE a través de un sistema común de identificación de datos para los visados a corto plazo en todos los estados miembros[3]. El VIS opera a través de un sistema centralizado llamado *Central Visa Information System* (CS-VIS), conectado a una interfaz nacional en cada Estado miembro (NI-VIS) mediante una infraestructura de comunicación entre CS-VIS y NI-VIS (artículo 1(2) de la Decisión VIS). La Decisión VIS fue implementada a través de un reglamento en el año 2008 (Comunidades Europeas, 2008: 61-81) que constata que los objetivos principales del VIS son los siguientes: i) facilitar el procedimiento de solicitud de visados; ii) prevenir el llamado «*shopping* de visados»; iii) favorecer la lucha contra el fraude; iv) fomentar los controles en fronteras exteriores entre estados miembros; v) ayudar en la identificación de personas con acceso denegado en territorio de los

3. Reino Unido, Irlanda y Dinamarca no tomaron parte en su adopción, e Islandia y Noruega implementaron la Decisión como parte del acervo Schengen.

estados miembros; vi) facilitar la aplicación del Reglamento Dublín II (Comunidades Europeas, 2003: 1-10), y vii) contribuir en la prevención de amenazas a la seguridad interna de algunos de los estados miembros (artículo 2 del Reglamento VIS).

La Decisión del Consejo de 2008 (Consejo de la UE, 2008b: 129-136) amplió el artículo 3 del anterior Reglamento VIS al permitir el acceso de los datos VIS a entes policiales[4]. Así, además de las autoridades de inmigración y asilo, y los entes responsables de realizar controles en fronteras externas, la Decisión del Consejo de 2008 permite que cuerpos de policía de los estados miembros, la Europol, algunas autoridades en terceros países y determinadas organizaciones internacionales puedan acceder a los datos. Todos ellos obtuvieron este acceso a partir del 1 de septiembre de 2013 (Statewatch, 2013). El VIS empezó a ser operativo en 2011 (Comisión Europea, 2011) y procesó un millón de solicitudes durante el primer año (Steria, 2012); durante los años 2012 y 2013 esta cifra subió a más de cuatro millones (Consejo de la UE, 2014a: 3). El sistema VIS sigue expandiéndose año tras año: en 2012 y 2013 aumentó su competencia por todo el continente africano, Oriente Próximo y la región del Golfo, y se espera que llegue a cubrir todo el mundo a finales de 2015 (Consejo de la UE, 2014a: 3-4).

Por otro lado, el Sistema de Información Aduanera (CIS) tiene su origen en el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros (Consejo de la UE, 1995: 33-47) y el Convenio relativo a la asistencia mutua y la cooperación entre las administraciones aduaneras (Consejo de la UE, 1998: 1-22). Estos dos convenios se crearon para luchar contra el tráfico ilegal. El CIS se firmó en 1995 pero no entró en vigor hasta el año 2005, después de ser ratificado por todos los estados miembros. Antes del Tratado de Lisboa, se aprobó otro instrumento europeo para intercambiar los datos aduaneros. Se trataba de un reglamento adoptado bajo el marco del antiguo primer pilar, que recogía información sobre personas para fines específicos de observación e información, vigilancia discreta y controles concretos en el ámbito agrícola y aduanero. Los datos CIS también se utilizan actualmente con fines policiales. Además del CIS *tradicional*, que se estableció gracias al Reglamento 766/2008, que formaba parte del anterior primer pilar, en 2008 se adoptó una Decisión del Consejo (Decisión CIS) dentro del marco del tercer pilar (Consejo de la UE, 2009: 20-30). La

4. Cabe destacar que las agencias policiales de Irlanda y Reino Unido fueron excluidas del acceso a los datos VIS porque estos países no formaban parte de Schengen. En el asunto C-482/08, el Reino Unido impugnó sin éxito la exclusión, en la que el TJUE finalmente determinó que no era un error el hecho de dejar a estos estados miembros fuera del alcance de la Decisión del Consejo.

finalidad principal de la Decisión CIS era asistir en la prevención, investigación y persecución de delitos graves según las leyes nacionales al proporcionar información de manera rápida (artículo 1(2) de la Decisión CIS). Según el artículo 5 de la Decisión CIS, los datos que entran en el sistema son usados para fines de observación y denuncia, vigilancia discreta, controles específicos, así como análisis estratégicos y operativos. Por ejemplo, uno de los casos habituales en el que se intercambian datos CIS entre entes policiales o de aduanas es el que tiene relación con delitos de tráfico de armas (Consejo de la UE, 2010a). La Decisión CIS incluye la regulación de la base de datos de identificación de archivos de aduana o FIDE (artículo 25 de la Decisión CIS). La FIDE permite a las autoridades aduaneras, a Europol y a Eurojust identificar las entidades competentes en otros estados miembros para investigar casos destinados a una persona física o jurídica. La información solo se obtiene si el caso tiene relación con un delito grave con pena de al menos 12 meses de prisión o bien una sanción administrativa de como mínimo 15.000 euros (artículo 15(1) de la Decisión CIS). La Comisión es la institución que controla la recogida de información, incluidos datos personales, según las siguientes categorías: mercancías, medios de transporte, negocios, personas, casos de fraude, disponibilidad de conocimientos, objetos retenidos o confiscados, y dinero retenido o confiscado (artículo 3(2) de la Decisión CIS).

Finalmente, con respecto a los datos de los solicitantes de asilo, 12 estados miembros firmaron en 1995 el convenio relativo a la determinación del Estado responsable del examen de las solicitudes de asilo presentadas en los estados miembros de las Comunidades Europeas (Convenio de Dublín). El examen se llevaba a cabo a través de un sistema centralizado que comparaba las huellas de los solicitantes de asilo. Recibió el nombre de Eurodac y su objetivo era ayudar a determinar qué Estado miembro era responsable de examinar una solicitud. Además, Eurodac también servía para prevenir casos de «*shopping* de asilo»[5] y «refugiados en órbita»[6]. Este sistema se reguló por primera vez en el año 2000 por un reglamento del Consejo que obligaba a todos aquellos países que hubieran implementado el acervo del Convenio de Dublín –es decir, todos los estados miembros más Islandia, Noruega, Suiza y Liechtenstein–. Eurodac inició sus operaciones en 2003 y consiste en un sistema centralizado que conecta los 28 puntos de acceso nacionales.

5. El «*shopping* de asilo» consiste en solicitar múltiples asilos de manera simultánea por la misma persona en diversos estados miembros.
6. «Refugiados en órbita» es la situación en la que todos los estados miembros reclaman que no son competentes para examinar una solicitud de asilo.

La primera propuesta para la reforma del Reglamento Eurodac fue publicada por la Comisión en diciembre de 2008 (Comisión Europea, 2008). Nueve meses más tarde, la Comisión, influenciada por el Consejo (Consejo de la UE, 2007), lanzó una nueva enmienda a esa propuesta en forma de paquete –un Reglamento y una Decisión del Consejo (Comisión Europea, 2009)– que introducía la posibilidad de que las agencias policiales de los estados miembros y Europol tuvieran acceso a la base de datos central de Eurodac para la prevención, detección e investigación de delitos graves. Así, la propuesta de Decisión del Consejo permitía a las autoridades policiales intercambiar huellas dactilares. Sin embargo, con motivo de la entrada en vigor del Tratado de Lisboa, la Comisión decidió eliminar las disposiciones de la propuesta que hacían referencia al acceso de datos por agencias policiales y presentó una nueva iniciativa en forma de Reglamento en 2010 (Comisión Europea, 2010b), similar a la de 2008. Esta propuesta de 2010 fue reemplazada por otra en mayo de 2012 (Comisión Europea, 2012), que incorporaba de nuevo en un único instrumento las disposiciones que permitían el acceso a los datos por agencias policiales. La nueva propuesta intentó acercarse a la regulación de las bases de datos SIS II y VIS, examinadas anteriormente, para identificar a sospechosos de terrorismo y delitos graves. Se aprobó en junio de 2013 (Unión Europea, 2013: 1-30), adquiriendo efectos en todos los estados miembros excepto Irlanda y Dinamarca[7]. Su puesta en marcha viene reforzada por las reformas aprobadas en el paquete de asilo de 2013 y por los nuevos desarrollos de *una cuota de asilo* iniciados en mayo de 2015 por la Comisión Europea.

Por lo tanto, los cuatro sistemas analizados tienen en común que han ido expandiendo su objetivo original con el fin de convertirse en herramientas para prevenir, detectar e investigar delitos. Es importante remarcar que todos ellos, excepto el CIS, están gestionados por una nueva agencia europea llamada EU-LISA, que entró en funcionamiento en diciembre de 2012. El objetivo de la agencia es asegurar que la información que se intercambia mediante estos sistemas tecnológicos sea segura y cumpla con la legislación de protección de datos. Así mismo, la agencia emite informes periódicos sobre aspectos técnicos tanto al Parlamento Europeo (PE) como al Consejo (artículo 50(3) del Reglamento VIS), e informes anuales de su actividad a las distintas delegaciones del Consejo (Consejo de la UE, 2014b). Esta centralización de la gestión de información en un solo organismo debe recibirse con optimismo. Ciertamente ha reforzado las relaciones entre los distintos sujetos del ELSJ y, probablemente, conllevará más coherencia en la regulación y funcionamiento de los diferentes sistemas de intercambio de información en el ámbito policial dentro de la UE.

7. El Reino Unido decidió formar parte del Reglamento Eurodac.

Legislación específica de protección de datos en el ámbito del ELSJ

A día de hoy no existe un marco jurídico unificado de protección de datos en el ámbito del ELSJ. De hecho, muchos de los intercambios de datos llevados a cabo por los cuerpos policiales de los estados miembros se encuentran aún sujetos exclusivamente a leyes penales nacionales. Según el artículo 3(2) de la Directiva 95/46/CE, las leyes europeas de protección de datos no son de aplicación en aquellos casos en los que el tratamiento de datos tenga un fin de seguridad pública, defensa, seguridad del Estado y actividades del Estado en el ámbito penal. Esta disposición se ha convertido en un obstáculo cada vez que la UE ha intentado incorporar un nuevo instrumento de intercambio de datos en el campo de la seguridad pública. Antes de 2008 la única solución era enmascarar este tipo de medidas bajo el paraguas del antiguo primer pilar, tal y como ocurrió con el acuerdo internacional para la recogida de datos de pasajeros entre las Comunidades Europeas y Estados Unidos en 2004 (Comunidades Europeas, 2004: 83), o la Directiva de Conservación de Datos adoptada en 2006 (Comunidades Europeas, 2006b: 54-63). En 2008 el paradigma cambió con la adopción de la Decisión Marco del Consejo sobre la protección de datos en asuntos policiales y judiciales, parte del antiguo tercer pilar. Aunque tal instrumento mejoró la situación de aquel momento, lo cierto es que la Decisión Marco 2008/977/JAI ha estado sujeta a muchas críticas por ser demasiado ambigua y dejar un margen de discreción muy amplio para la implementación de los estados miembros. Este apartado analiza el alcance y limitaciones de la Decisión Marco 2008/977/JAI (Consejo de la UE, 2008a: 60-71), para luego compararla con la propuesta para una directiva sobre protección de datos en el ámbito penal.

El alcance limitado de la Decisión Marco 2008/977/JAI

La Decisión Marco 2008/977/JAI (en adelante, la Decisión Marco) fue el primer instrumento de protección de datos adoptado como parte del antiguo tercer pilar de la UE. La necesidad de tener una ley europea que regulara los intercambios transfronterizos de datos entre agencias policiales se había destacado por primera vez en el Programa de La Haya cuatro años antes. La propuesta se redactó en 2005 (Comisión Europea, 2005) e incluía normas sobre los derechos de los individuos, organismos de supervisión, tratamiento de datos y transferencias de datos similares a las que se encontraban en la Directiva 95/46/CE. Sin embargo,

ese primer borrador se modificó sustancialmente a causa de la falta de precisión de algunas disposiciones (De Hert y Papakonstantinou, 2009: 407). La nueva propuesta no se lanzó hasta el año 2008.

La Decisión Marco se basa en los antiguos artículos 30(a) y (b) del Tratado de la Unión Europea (TUE) –hoy en día los artículos 87-88 del Tratado de Funcionamiento de la Unión Europea (TFUE)–. Su objetivo principal es asegurar que los datos que se intercambian entre estados miembros cumplen con unos estándares elevados de protección de datos a la vez que garantizan un buen mantenimiento de la seguridad pública (artículo 1(1) de la Decisión Marco 2008/977/JAI). La Decisión Marco incluía normas de protección de datos como la legalidad y proporcionalidad en el tratamiento de datos; el principio de limitación de la finalidad, precisión en el tratamiento de datos; derechos a borrar, eliminar y bloquear los datos personales; medidas técnicas adecuadas contra la destrucción, pérdida, alteración o acceso no autorizado de datos personales; normas de confidencialidad y seguridad de los datos; compensación, responsabilidad y sanciones, y la obligación de una supervisión independiente (artículos 3(1), 6(1)(b), 4(1), 7, 8, 18, 19, 21, 22, 24 y 25). Las autoridades policiales deberían cumplir con esta ley cada vez que transfirieran datos personales a otro Estado miembro para prevenir, investigar, detectar o perseguir un delito penal (considerando 6 de la Decisión Maro 2008/977/JAI). No obstante, este instrumento no es de aplicación en aquellas situaciones puramente internas en las cuales la información se recoge y usa por un único Estado miembro. Esta fue una de las críticas que recibió la Decisión Marco después de su adopción (De Hert y Bellanova, 2009: 6). Otro aspecto criticado fue la naturaleza elegida. Dado que se trataba de una Decisión Marco, la Comisión no tenía medios para obligar a los estados miembros a que cumplieran con ella.

No existe un marco jurídico unificado de protección de datos en el ámbito del ELSJ. Muchos de los intercambios de datos llevados a cabo por los cuerpos policiales de los estados miembros se encuentran aún sujetos exclusivamente a leyes penales nacionales.

El hecho de que los principios de la Decisión Marco 2008/977/JAI no fueran completamente equivalentes a los de la Directiva 95/46/CE también fue otro aspecto muy debatido (De Hert y Papakonstantinou, 2009; De Hert y Bellanova, 2009: 6-7; Boehm, 2012: 138-144; Hijmans y Scirocco, 2009: 1.494). Por ejemplo, la Decisión Marco no incluye ningún artículo que prohíba el tratamiento de datos sensibles, sino que el propio artículo 6 de dicho instrumento establece que los datos relativos a la raza, política, creencias filosóficas o religiosas, participación en sindicatos, salud o vida sexual de una

persona podrán tratarse siempre que sea estrictamente necesario y bajo unas garantías adecuadas[8]. Otra diferencia se encuentra en la condición de notificación e información al individuo. En concreto, el párrafo 27 de la Decisión Marco establece excepciones a esa norma general de notificación, las cuales no se encuentran en la Directiva. Además, así como la Directiva prevé un derecho de oposición del individuo cuyos datos son tratados, un derecho similar no se recoge en la Decisión Marco (artículo 13 de la Decisión Marco 2008/977/JAI). Finalmente, ambos instrumentos especifican poderes para autoridades de protección de datos independientes; sin embargo, ningún organismo de supervisión similar al Grupo del Artículo 29[9] se encuentra regulado en el texto de la Decisión Marco.

La mayor decepción respecto al contenido de la Decisión Marco 2008/977/JAI fue la exclusión de determinados instrumentos sectoriales de la UE del marco de la Decisión (considerando 39). Concretamente, la Decisión Marco no se aplica en aquellos casos de tratamiento de datos por parte de Europol, Eurojust, el SIS, el CIS, el sistema Prüm[10], todos los acuerdos internacionales de tratamiento de datos con terceros estados (por ejemplo, los acuerdos PNR)[11] y otros actos legislativos de la UE que permiten el intercambio de información en el ámbito penal (artículo 28). Aunque estos instrumentos ya tienen sus propias cláusulas de protección de datos y, además, se basan en los principios del Consejo de Europa, un régimen general por parte de la Decisión Marco 2008/977/JAI habría asegurado un umbral de protección mínima para todos los sistemas europeos de información. Todas estas limitaciones comportaron la necesidad de redactar un nuevo acto legislativo a nivel europeo para la protección de datos en materia policial y judicial, especialmente después de la entrada en vigor del Tratado de Lisboa.

8. Es interesante el hecho de que Europol, la cual está excluida del alcance de la Decisión Marco 2008/977/JAI, ofrezca más garantías de protección de datos, ya que el artículo 10 de la Decisión del Consejo sobre Europol no permite el tratamiento de datos que revelen la raza o etnia, opiniones políticas, religiosas o filosóficas, participación en sindicatos o bien datos de salud o vida sexual.
9. Este grupo se creó en 1996 y se encarga de publicar opiniones sobre cuestiones de protección de datos en el marco de la Directiva 95/46/CE. Se compone por una autoridad de protección de datos de cada estado miembro, el Supervisor Europeo de Protección de Datos y la Comisión Europea.
10. La Decisión Prüm establece un marco legal de cooperación entre los entes policiales de los estados miembros. Concretamente, permite intercambiar datos relacionados con huellas digitales, ADN y registro de vehículos.
11. Son acuerdos internacionales que la UE ha firmado con Estados Unidos, Australia y Canadá y que obligan a las compañías aéreas a suministrar datos de todos los pasajeros procedentes de vuelos europeos a las autoridades policiales de estos tres países.

Propuesta para una directiva relativa al tratamiento de datos personales para la cooperación policial y judicial en asuntos penales

La Decisión Marco 2008/977/JAI no cumple con los criterios del artículo 16 del TFUE, ya que no es de aplicación en las actividades de tratamiento de datos personales puramente internas y, además, excluye la participación del PE (Hijmans y Scirocco, 2009: 1.519; De Hert y Bellanova, 2009: 7). Por eso, cuando el Tratado de Lisboa entró en vigor, surgió la necesidad de modificar o reemplazar la Decisión Marco 2008/977/JAI. En este sentido, la Declaración 21 adjunta al Tratado de Lisboa permite a la UE adoptar normas específicas sobre protección de datos en el sector policial y judicial, teniendo en cuenta la naturaleza específica de estas áreas.

El Programa de Estocolmo fue la primera iniciativa post-Lisboa que determinó la nueva legislación en el ámbito del ELSJ, incluyendo el tratamiento de la información con finalidades de seguridad[12]. Más tarde, El Consejo Europeo y la Comisión concretaron lo previsto en el programa a partir de una comunicación (Comisión Europea, 2010c) y una estrategia (Consejo Europeo, 2010), con el fin de establecer normas de protección de datos dentro del ELSJ. La comunicación publicada por la Comisión fue el primer paso para crear un nuevo marco de protección de datos dentro de la UE. Esta subrayó los nuevos retos surgidos de los rápidos avances tecnológicos, junto con la falta de armonización de leyes sobre protección de datos en la UE y los inadecuados regímenes para la transferencia de datos con terceros estados. Además, la Comisión propuso una serie de compromisos clave como el incremento de la transparencia, más control de los individuos sobre sus datos personales, refuerzo de las normas de consentimiento, armonización de las condiciones de tratamiento de datos sensibles y establecimiento de sanciones y recursos eficaces. Igualmente, la Comisión mencionó la necesidad de revisar las normas de protección de datos en el área de la cooperación policial y judicial en asuntos penales. Esta comunicación se materializó el 25 de enero de 2012 cuando la Comisión publicó dos propuestas legislativas: la propuesta para un Reglamento General de Protección de Datos y la propuesta para la Directiva de Protección de Datos en el ámbito Policial y de Justicia Penal (Comisión Europea, 2012b). Este estudio se centra solamente en la propuesta de Directiva.

12. Sin embargo, el Programa de la Haya de 2004 ya incluía el intercambio de información como uno de los objetivos clave en los siguientes cinco años. También preveía el incremento de recogida e intercambio de información con el objetivo de gestionar los desplazamientos migratorios así como controlar y prevenir delitos. Véase DO C 53, 03.03.2005, p. 1-14.

La propuesta de Directiva reemplazará a la actual Decisión Marco 2008/977/JAI (artículo 58 de la propuesta de Directiva). Si comparamos los dos instrumentos, se puede comprobar que la propuesta incluye una mejora respecto a la ley actual. Por ejemplo, la primera confiere efecto directo a los individuos, se somete a la Carta de Derechos Fundamentales de la UE, cuenta con la participación del PE en el procedimiento legislativo y entra en el campo de jurisdicción del Tribunal de Justicia de la UE (TJUE) (Peers, 2012: 2-3). Así, cualquier juez nacional puede referir una cuestión prejudicial sobre datos tratados por fines policiales al TJUE. En cuanto al contenido, la propuesta amplía el alcance de la aplicación de la Decisión Marco 2008/977/JAI: ya no solo se aplica a aquellas actividades transfronterizas de intercambio de datos, sino que también cubrirá el tratamiento de datos en el ámbito estrictamente nacional. Sin embargo, algunos estados miembros se han opuesto a esta novedad, argumentando que la regulación del tratamiento de datos a nivel nacional podría ir en contra del principio europeo de subsidiariedad[13]. Otros han expresado dudas sobre la viabilidad de la propuesta puesto que pretende armonizar las leyes de protección de datos en el ámbito policial (Consejo de la UE, 2013b: 4), o simplemente consideran que la actual Decisión Marco 2008/977/JAI es suficiente (Consejo de la UE, 2013c: 2).

La propuesta de Directiva incluye algunas mejoras con respecto a los derechos de los individuos, como la obligación de notificarles que sus datos personales son tratados (artículo 11 de la propuesta de Directiva). Sin embargo, existen aún muchas excepciones con respecto al derecho a ser informados (artículo 11(4) y (5) de la propuesta de Directiva) y el derecho de acceso a sus datos personales (artículo 13 de la propuesta de Directiva). En este sentido, el Grupo del Artículo 29 ha sugerido que se elimine de la propuesta la posibilidad de excluir categorías enteras de datos de estos derechos (Grupo del Artículo 29, 2013a: 3). Así mismo, se debe hacer hincapié en el artículo 5 de la propuesta sobre los diferentes procedimientos de tratamiento de datos según la categoría de los individuos a cuyos datos se accede (sospechosos, condenados, víctimas, testigos, contactos o personas asociadas, entre otros). Además, el artículo 8(1) establece que los datos clasificados como sensibles[14] en principio no podrán ser tratados. Esta disposición ha ocasionado mucho debate a nivel nacional, ya que muchas autoridades nacionales de los estados miembros advierten que los datos sensibles pueden ser

13. Según el principio de subsidiariedad, definido en el artículo 5(3) del TUE, los estados miembros serán los encargados de regular aspectos dentro del ámbito de las políticas compartidas de la UE siempre y cuando estos estén más cualificados que la UE para legislar sobre dichos ámbitos.
14. Los datos sensibles son aquellos datos personales que revelan el origen étnico o racial, opiniones políticas, creencias religiosas, participación en sindicatos, datos genéticos o datos de vida sexual.

muy relevantes para una investigación penal y que, por lo tanto, este artículo debería suprimirse (Consejo de la UE, 2013b: 6). De hecho, la mayoría de los estados miembros prefieren el redactado de la Decisión Marco 2008/977/JAI, ya que no está formulado como una prohibición.

Aunque la propuesta de Directiva mejora la actual Decisión Marco, hay muchos aspectos que han sido recibidos con decepción por parte de la comunidad de expertos de protección de datos. Uno de los temas más polémicos tuvo que ver con la propuesta que se filtró en noviembre de 2011, dos meses antes de que se publicara la versión de propuesta oficial por la Comisión. En aquel primer borrador aparecían mayores garantías de protección de datos que las que finalmente se incluyeron en la versión final de propuesta (Bäcker y Hornung, 2012: 628). Por ejemplo, la propuesta oficial no contiene mención alguna de las llamadas evaluaciones de impacto de protección de datos, que sí aparecían en el borrador filtrado (ibídem: 629). Otra crítica se refiere a la supresión del artículo 1(5) de la Decisión Marco 977/2008/JAI. Esta cláusula prevé que la Decisión Marco no impida que los estados miembros puedan adoptar estándares más altos de protección de datos que los establecidos a nivel europeo. Un artículo equivalente no se encuentra en la propuesta de Directiva, a pesar de que algunos estados miembros ya han expresado públicamente su voluntad de ofrecer garantías de protección de datos más altas a nivel nacional que las que incluye la propuesta (Consejo de la UE, 2013b: 3). Otro descontento entre la comunidad a favor de la protección de datos lo han ocasionado las normas de conservación de datos personales en la propuesta. Concretamente, el artículo 24 establece que se permitirá la identificación personal mediante el tratamiento de datos personales «en la medida de lo posible». Esta ambigüedad viene reforzada por el artículo 4(e) de la propuesta, que establece lo siguiente: «[Los datos deben ser] conservados en una forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que se someten a tratamiento».

El riesgo que puede derivarse de este redactado es que la información termine usándose para múltiples procedimientos de investigación sin ningún tipo de limitación temporal (Consejo de la UE, 2013b: 5). En este contexto, la reciente anulación de la Directiva de Conservación de Datos (TJUE, 2014) ha despertado mucho debate en relación con la falta de normas precisas sobre la cooperación entre entes públicos y privados, medidas de *profiling*[15], así como la necesidad de definir el término «delito grave» en la propuesta. Tal y como

15. El *profiling* en el ámbito penal consiste en utilizar los datos compilados sobre personas que han cometido un delito con el objetivo de describir o identificar los grupos de personas que pueden ser sospechosos de un delito.

ya han sugerido algunos académicos, la propuesta debería ser revisada a la luz de los argumentos del TJUE en el asunto de la Directiva de Conservación de Datos (Boehm y Cole, 2014: 85-87).

A pesar de que la inclusión de una autoridad independiente de supervisión supone un gran avance, este tendrá poderes limitados. Por ello, el Grupo del Artículo 29 ha recomendado ampliar el artículo 46 sobre los poderes de las autoridades de supervisión y añadir la posibilidad de acceder a todos los documentos necesarios para el ejercicio de sus investigaciones (Grupo del Artículo 29, 2013a: 7). Esta modificación ofrecería una supervisión completa en el tratamiento de datos dentro del ámbito policial y judicial, equivalente a la que encontramos actualmente en la Directiva 95/46/CE. Así mismo, el hecho de que la propuesta no haya sido adoptada en forma de reglamento ha comportado críticas entre varios sectores defensores de la protección de datos en la UE. Concretamente, el Supervisor Europeo de Protección de Datos (SEPD, 2012a: iv), el Grupo del Artículo 29 (Grupo del Artículo 29, 2013a: 26) y el PE (Parlamento Europeo, 2012) han expresado su descontento por ello y han puesto de manifiesto que el nivel de protección de datos que ofrece la propuesta de Directiva es inadecuado, ya que es muy inferior al de la propuesta para un Reglamento General de Protección de Datos. Contrariamente, algunos estados miembros han considerado que los dos instrumentos propuestos como paquete de reforma de la normativa europea de protección de datos debería haberse adoptado en forma de directiva, ya que la situación actual puede crear solapamientos entre los dos actos legislativos (Consejo de la Unión Europea, 2013c: 2). Al final, la separación de instrumentos (un reglamento y una directiva) parece que no sufrirá modificaciones. La Comisión ha justificado la elección de instrumentos diferentes según la Declaración 21 del Tratado de Lisboa, la cual reconoce que se podrán adoptar normas específicas de protección de datos en el ámbito penal. Además, la mayoría de estados miembros se decantó desde un principio por la naturaleza de directiva debido a que no quieren ceder más competencias a la UE en el ámbito penal.

La propuesta de Directiva no especifica si se aplicará en los casos en que los datos sean recogidos por entes privados para finalidades de mercado interior, aunque posteriormente sean accesibles para las autoridades policiales. En mi opinión, dependerá de quién sea el sujeto que lleve a cabo el tratamiento de datos. Si es realizado por un ente público, entonces se aplicará la propuesta de Directiva; pero si la encargada del tratamiento es la compañía privada, el instrumento aplicable será la propuesta de Reglamento. En este sentido, el Consejo ha aclarado que si una entidad privada recoge datos personales para finalidades comerciales y está obligada a proporcionarlos posteriormen-

te a agencias policiales, se tendrán que seguir las normas de la propuesta de Reglamento (por ejemplo, datos almacenados por compañías proveedoras de servicios de telecomunicaciones, compañías aéreas o entidades financieras) (Consejo de la UE, 2014c: 5).

El artículo 2(3) de la propuesta de Directiva excluye explícitamente del alcance de aplicación la información tratada por instituciones, agencias u organismos europeos. Esto significa que, por ejemplo, datos tratados por Europol no entran dentro del alcance de la propuesta. En consecuencia, la divergencia de marcos jurídicos de protección de datos en el ámbito del ELSJ permanecerá en el futuro. La propuesta de Directiva podría haber servido para establecer un umbral mínimo de normas de protección de datos en el ámbito de cooperación policial y judicial, pero no ha sido así. En conclusión, a pesar de que la propuesta ofrece una mejora en cuanto a las normas europeas de protección de datos en el ámbito penal, no he conseguido poner punto y final a la fragmentación de normas que existe actualmente. Cuando la propuesta de Directiva entre en vigor aún seguirán habiendo diversos sistemas de información europeos que quedarán fuera del alcance de ese instrumento legislativo, lo cual significa que no se conseguirá una armonización de las normas de protección de datos en el ámbito policial y judicial.

Protección de datos en SIS/SIS II, VIS, Eurodac y CIS

Tal y como se ha visto anteriormente, tanto la actual Decisión Marco 2008/977/JAI como la propuesta de Directiva de protección de datos para asuntos policiales y judiciales excluyen muchos de los instrumentos de derecho derivado que ha ido adoptando la UE para permitir el intercambio de datos personales. La razón de tal exclusión es principalmente política, ya que muchos estados miembros consideraron que centralizando las normas de protección de datos en un único acto legislativo perderían sus competencias en la regulación de medidas en el ámbito de la seguridad colectiva. Tanto la Decisión Marco como la propuesta de Directiva incluyen una cláusula que prevé que las normas anteriores sobre protección de datos prevalecerán a estos actos legislativos (artículo 28 de la Decisión Marco 2008/977/JAI y artículo 59 de la propuesta de Directiva). Igualmente, si existen normas específicas más restrictivas sobre protección de datos, estas también tendrán un carácter preferente (considerando 40 de la Decisión Marco 2008/977/JAI).

La mayoría[16] de los instrumentos europeos para el intercambio de datos en el ELSJ contienen ya sus propias cláusulas de protección de datos. Algunos de estos instrumentos son medidas preventivas que se dedican a almacenar datos de todos los ciudadanos, como es el caso del SIS/SIS II, el VIS, Eurodac y el CIS. El principal problema de estos instrumentos es que sus respectivas normas de protección de datos no coinciden. La tabla que se presenta a continuación compara estos sistemas europeos de información y analiza cuatro criterios diferentes: la conservación de datos, las categorías de datos recogidos, las entidades que pueden acceder a estos datos y los derechos individuales que se garantizan.

Lo primero que se puede observar en esta tabla es que ninguno de los sistemas europeos de información coincide con respecto a sus normas de protección de datos. La conservación de información va de dos a diez años. Después de que el TJUE declarase nula la Directiva de Conservación de Datos, hay una conclusión clara que se desprende de esta tabla: todos los instrumentos analizados tienen períodos de conservación iguales o superiores al de la directiva anulada, que preveía retenciones de entre seis meses y dos años. Por ello, siguiendo el argumento del TJUE, estos períodos podrían considerarse contrarios a los principios de necesidad y proporcionalidad de la UE (Boehm y Cole, 2014: 67-68 y 80). En cuanto al número de categorías de datos recogidas, estas también varían de manera significativa de un instrumento a otro. Por ejemplo, el CIS recoge 14 categorías de datos, mientras que el VIS recoge 32 tipos de datos distintos. En todos los casos se revela un número considerable de datos de los ciudadanos, que puede percibirse como una intrusión en la vida personal de las personas (ibídem: 69), similar a la que determinó el TJUE al anular la Directiva de Conservación de Datos, ya que se contradecía el artículo 7 de la Carta de Derechos Fundamentales de la UE.

Respecto a las autoridades e instituciones con acceso a la información, cada uno de los instrumentos analizados incluye autoridades distintas, que pueden pertenecer a cuerpos de policía nacionales o incluso a Europol y Eurojust. El problema principal que puede surgir de estas categorías tan amplias con acceso a los datos es precisamente que permite que un número muy elevado de personas obtenga los datos introducidos en los sistemas. Por ejemplo, no está claro quiénes son las «autoridades de verificación» que se describen en el reglamento de Eurodac. Tal y como mencionan Boehm y Cole (2014: 70, 79), esta imprecisión deja margen a la posible expansión arbitraria de personas que pueden acceder al conjunto de datos; por lo tanto, proponen designar

16. Este no es el caso de la Decisión del Consejo 2005/671/JAI de 20 de septiembre de 2005 relativa al intercambio de información y a la cooperación sobre delitos de terrorismo, DO L 253, 29.09.2005, p. 22-24.

un organismo independiente de supervisión en todos los cuerpos policiales que controle este acceso. Finalmente, los derechos garantizados para los individuos en todos los instrumentos analizados para este estudio se pueden considerar insuficientes si los comparamos con los que incluye la Directiva 95/46/CE. Esta directiva establece que todo individuo tendrá derecho a acceder, suprimir, corregir, bloquear, recurrir judicialmente y recibir compensación por la incorrecta utilización de sus datos. La lista completa de garantías no se encuentra en ninguno de los sistemas.

Tabla 1. Comparativa de sistemas europeos de información

	Conservación de datos	Categorías de datos recogidos	Entidades con acceso a los datos	Derechos de los ciudadanos
SIS/SIS II	5 o 10 años máximo; revisión después de 1 o 3 años	10/15	Autoridades de frontera; autoridades de aduana y policiales; autoridades judiciales; autoridades de visado e inmigración; Europol y Eurojust; autoridades de registro de vehículos; Interpol	Acceso, supresión, modificación, recurso judicial, compensación
VIS	5 años máximo	34	Autoridades de frontera; autoridades de visado e inmigración; autoridades policiales; Europol; terceros estados y organizaciones internacionales.	Acceso, supresión, modificación, recurso judicial
Eurodac	10 años o 2 años	12	Autoridades nacionales de asilo; autoridades policiales	Acceso, supresión, modificación, recurso judicial, compensación
CIS	3 años, 6 años o 10 años máximo; revisión después de 1 año	14	Administraciones de aduana; otras autoridades nacionales; terceros estados y organizaciones internacionales/ regionales	Acceso, supresión, modificación, bloqueo

Fuente: Elaboración propia.

Principios de limitación de finalidad y necesidad

Hay dos principios de protección de datos que se han visto afectados especialmente por la creciente instalación de sistemas de intercambio de datos en la UE para fines policiales: el principio de limitación de finalidad y el principio de necesidad.

Observando primero el principio de limitación de finalidad, este se encuentra definido en el artículo 6(1)(b) de la Directiva 95/46/CE. Según el Grupo del Artículo 29 (2013b), el principio de limitación de finalidad consiste en recoger datos personales para finalidades específicas, explícitas y legitimadas, que no pueden ser tratados de manera incompatible con la finalidad original. Este principio se ha visto perjudicado por la progresiva desviación de uso en los sistemas de información europeos, que se puede definir como la ampliación gradual en el uso de un sistema o base de datos más allá de su finalidad original (SEPD, 2012b: 5). Este hecho se ha producido en todos los sistemas que se han examinado en este estudio: el SIS, el VIS, Eurodac y el CIS se crearon inicialmente para controlar las fronteras europeas o para fines comerciales, pero se han tratado posteriormente como una herramienta de detección e investigación de un delito. Por ejemplo, el VIS fue creado para reforzar la política común de visados y Eurodac se estableció para prevenir que los solicitantes de asilo enviaran múltiples solicitudes de manera simultánea a varios estados miembros. No obstante, los datos recogidos por estos sistemas son ahora también accesibles para agencias policiales de los estados miembros y Europol para combatir el terrorismo y otros delitos graves. Así, una vez la información se recoge y almacena en estos sistemas centralizados, se permite su uso al sector policial. En este sentido, el Grupo del Artículo 29 (2013b: 68-69) ha considerado que todos los sistemas objeto de este estudio son incompatibles con el principio de limitación de finalidad de la UE.

Al examinar los límites de la desviación de uso de los datos personales, según el Grupo del Artículo 29, debe tenerse en cuenta el principio de necesidad. En todos los actos que regulan los sistemas vistos arriba (SIS/SIS II, VIS, Eurodac y CIS) hay una cláusula que establece que estos cumplen con los criterios de necesidad y proporcionalidad. El Grupo del Artículo 29 ha remarcado que es posible restringir el principio de limitación de finalidad si ello es estrictamente necesario para salvaguardar ciertos intereses de gran importancia (artículo 13 de la Directiva 95/46/CE). Sin embargo, el problema es que no existen parámetros estrictos para evaluar la necesidad de que las agencias policiales accedan a los datos almacenados en sistemas de información de la UE. Por eso, para llevar a cabo un examen objetivo de la necesidad y proporcionalidad, se debería fomentar

el uso de evaluaciones de impacto para determinar tal acceso. Lamentablemente, la Comisión no siempre ha adjuntado evaluaciones de impacto antes de adoptar o reformar sistemas de información en la UE. Por ejemplo, la propuesta para reformar el reglamento de Eurodac en mayo de 2012 no incluía ninguna evaluación de impacto. El SEPD fue el primer organismo en reaccionar frente a este hecho y se quejó de que la Comisión no había demostrado suficientemente que las huellas dactilares de los solicitantes de asilo podían ser necesarias para investigaciones policiales. Por eso, el SEPD pidió a la Comisión que proporcionara pruebas sólidas y estadísticas fiables sobre la necesidad de acceder a los datos de Eurodac. La Autoridad Común de Control de Europol (ACC) también publicó un informe en octubre de 2012 en el que se analizaba este aspecto sobre el acceso a los datos de Eurodac. El informe determinó que había falta de pruebas de que ese acceso fuera necesario y proporcionado para combatir el terrorismo y otros delitos graves (ACC, 2012). Así, la ACC pidió que se realizara una evaluación precisa con la que se pudiera demostrar que tanto la autoridades policiales nacionales como Europol necesitaban acceder a esos datos. Después de ese informe, no es casualidad que el Consejo publicara un documento con ejemplos reales en los que la comparación de huellas dactilares recogidas en escenas de crímenes con aquellas recogidas en Eurodac habían contribuido positivamente a investigaciones criminales (Consejo de la UE, 2012b). De hecho, se ha podido comprobar que los estados miembros son los principales interesados en impulsar la desviación del uso de datos personales a finalidades policiales.

Hay dos principios de protección de datos que se han visto afectados especialmente por la creciente instalación de sistemas de intercambio de datos en la UE para fines policiales: el principio de limitación de finalidad y el principio de necesidad.

El TJUE (2014: par. 58) anuló la Directiva de Conservación de Datos precisamente porque la necesidad de retener datos personales no quedaba suficientemente justificada. El argumento del tribunal fue que la interferencia se aplica «incluso a personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con delitos graves». Dicho tratamiento de datos de personas que no son inicialmente sospechosas de un delito también ocurre con respecto a los otros instrumentos objeto de este estudio. Por ello queda por ver si el hecho de que el TJUE haya adquirido jurisdicción para decidir sobre medidas del antiguo tercer pilar desde diciembre de 2014 tendrá algún impacto en la práctica. Podría ocurrir que, siguiendo la misma argumentación del asunto de la Directiva de Conservación de Datos, otros instrumentos de intercambio de datos –incluidos el SIS/SIS II, el VIS, Eurodac y el CIS– pudieran ser impugnados en el futuro.

Conclusiones

En los últimos 15 años, la UE ha contribuido de manera relevante a la adopción de nuevos instrumentos para la prevención y lucha contra el terrorismo y otros delitos graves. Este estudio ha analizado la evolución de los sistemas de información SIS/SIS II, el VIS, Eurodac y el CIS que la UE instauró inicialmente para controlar las fronteras europeas. Con el paso del tiempo, estos sistemas de información han ido permitiendo el acceso a datos a las agencias policiales de los estados miembros y a Europol.

Este estudio también ha investigado las leyes europeas de protección de datos a las que quedarían sujetas las agencias policiales que utilizaran los datos de estos cuatro sistemas de información. Concretamente, se han analizado y comparado la Decisión Marco 2008/977/JAI y la propuesta de Directiva relativa a la protección de datos en el ámbito policial y judicial. Aunque la propuesta de Directiva introduce mejoras respecto a la ley actual –como el hecho de que cubra transferencias de datos puramente internas, un mayor papel del Parlamento Europeo y la posibilidad de revisión por parte del TJUE–, estas se han considerado insuficientes por parte de los expertos en el sector de la privacidad. El mayor descontento que ha provocado la propuesta de Directiva tiene que ver con el limitado alcance del instrumento. La propuesta excluye datos tratados por agencias de la UE como Europol y Eurojust, datos recogidos por el SIS y el CIS, así como datos almacenados por compañías privadas y posteriormente utilizadas por entidades policiales. Así mismo, se han comparado los artículos que regulan la protección de datos en el SIS/SIS II, el VIS, Eurodac y el CIS. Si bien todos los instrumentos de información estudiados contienen sus propias disposiciones de protección de datos, no existe armonización alguna en cuanto a dichas cláusulas ni tampoco una ley europea que cubra todos estos sistemas.

A la luz de este análisis, se puede concluir que hay demasiados marcos legislativos sobre protección de datos que convergen en el ámbito del ELSJ. Esta fragmentación dificulta la posibilidad de establecer estándares comunes de protección de datos y propicia el riesgo de que el TJUE acabe por determinar que estos sistemas de información europeos no cumplen con los principios de necesidad y limitación de finalidad.

Referencias bibliográficas

ACC-Autoridad Común de Control de Europol. «Opinion with respect to the European Commission's amended proposal for a Regulation of the European Parliament and of the Council on the establishment of EURODAC». *Opinión*, n.º

52 (10 de octubre de 2012) (en línea) [Fecha de consulta 12.05.2015] http://www.europoljsb.europa.eu/media/224155/12-52%204%20opinion%20on%20eurodac%20regulation.pdf

Bäcker, Matthias y Hornung Gerrit. «Data processing by police and criminal justice authorities in Europe - The influence of the Commission's draft on the national police laws and laws of criminal procedure». *Computer Law & Security Review*, vol. 28 n.º 6 (diciembre de 2012), p. 627-633.

Baldaccini, Anneliese. «Counter-Terrorism and the EU strategy for border security: Framing suspects with biometric documents and databases». *European Journal of Migration and Law*, vol. 10, n.º 1 (enero de 2008), p. 31-49.

Boehm, Franziska. *Information Sharing and Data Protection in the Area of Freedom, Security and Justice Towards Harmonised Data Protection Principles for Information Exchange at EU-level*. Berlín: Springer, 2012, p. 427.

Boehm, Franziska y Cole, Mark D. «Data Retention after the Judgement of the Court of Justice of the European Union». *Greens/EFA Group, European Parliament* (junio de 2014) Bruselas, p. 107.

Comisión Europea. «Proposal for a Council framework decision on the exchange of information under the principle of availability». COM(2005) 490 final (12.10.2005).

Comisión Europea. «Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]». COM(2008) 825 final (3.12.2008).

Comisión Europea. «Propuesta modificada del Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema EURODAC para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (CE) n.º […/…] [por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida]». COM(2009) 342 final y COM(2009) 344 final (10.09.2009).

Comisión Europea. «Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions of 4 November 2010 - A comprehensive approach on personal data protection in the European Union». COM(2010) 609 final (4.11.2010a).

Comisión Europea. «Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of EURODAC for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version)». COM(2010) 555 final (11.10.2010b).

Comisión Europea. «Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions -A comprehensive approach on personal data protection in the European Union». COM(2010) 609 final (4.11.2010c).

Comisión Europea. «More efficient and secure visa system goes live». *European Commission Press Release* (11.10.2011).

Comisión Europea. «Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)». COM(2012) 254 final (30.05.2012a).

Comisión Europea. «Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)» COM(2012) 11 final, COM(2012) 10 final (25.01.2012b).

Comunidades Europeas. «Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos». DO L 281 (23.11.1995), p. 31-50.

Comunidades Europeas. «Reglamento (CE) N.º 343/2003 de 18 de febrero de 2003 por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los estados miembros por un nacional de un tercer país». DO L 50 (25.02.2003), p. 1-10.

Comunidades Europeas. «Decisión del Consejo de 17 de mayo de 2004 relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados

Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos». DO L 183 (20.05.2004), p. 83.

Comunidades Europeas. «Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE». DO L 105 (13.04.2006), p. 54-63.

Comunidades Europeas. «Reglamento (CE) N º 767/2008 del Parlamento Europeo y del Consejo de 9 de julio de 2008 sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS)». DO L 218 (13.08.2008), p. 61-81.

Consejo de Europa. «Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal». *Serie de Tratados Europeos*, n.º 108 (28.01.1981).

Consejo de la UE. «Acto del Consejo 95/C316/02 de 26 de julio de 1995, por el que se establece el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros». DO C 316 (27.11.1995), p. 33-47.

Consejo de la UE. «Acto del Consejo, de 18 de diciembre de 1997, por el que se celebra, sobre la base del artículo K.3 del Tratado de la Unión Europea, el Convenio relativo a la asistencia mutua y la cooperación entre las administraciones aduaneras». DO C 24 (23.1.1998), p. 1-22.

Consejo de la UE. «Decisión del Consejo, de 8 de junio de 2004, por la que se establece el Sistema de Información de Visados (VIS)». DO L 213 (15.06.2004a), p. 5-7.

Consejo de la UE. «Reglamento del Consejo no 871/2004, de 29 de abril de 2004, relativo a la introducción de nuevas funciones para el Sistema de Información de Schengen, inclusive en materia de lucha contra el terrorismo». DO L 162 (30.04.2004b), p. 29-31.

Consejo de la UE. «Decisión 2005/211/JAI del Consejo, de 24 de febrero de 2005, relativa a la introducción de nuevas funciones para el Sistema de Información de Schengen, inclusive en materia de lucha contra el terrorismo». DO L 68, (15.03.2005), p. 44-48.

Consejo de la UE. Documento 5291/07 (12.01.2007).

Consejo de la UE. «Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal». DO L 350 (30.12.2008a), p. 60-71.

Consejo de la UE. «Decisión 2008/633/JAI del Consejo, de 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves». DO L 218 (13.08.2008b), p.129-136.

Consejo de la UE. «Decisión 2009/917/JAI del Consejo, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros». DO L 323 (10.12.2009), p. 20-30.

Consejo de la UE. Documento 16427/1/10 (29.11.2010).

Consejo de la UE. «Nota de la Delegación Francesa». Documento 8281/12 (28.03.2012a).

Consejo de la UE. Documento 16990/12 (3.12.2012b).

Consejo de la UE. Documento 7215/13 (7/8.03.2013a).

Consejo de la UE. Documento 14901/2/13 (30.10.2013b).

Consejo de la UE. Documento 11624/1/13 (2.10.2013c).

Consejo de la UE. Documento 7996/14 (21.03.2014a).

Consejo de la UE. Documento 11056/14 (7.07.2014b).

Consejo de la UE. Documento 11109/14 (30.06.2014c).

Consejo Europeo. «Internal Security Strategy for the European Union: Towards a European security model». Luxemburgo: Publications Office of the European Union (26.03.2010).

Grupo de Trabajo del Artículo 29. «Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive». WP 201 (26.02.2013a).

Grupo de Trabajo del Artículo 29. «Opinión 03/2013 sobre la limitación de finalidad». WP 203 (2.04.2013b).

De Hert, Paul y Papakonstantinou, Vagelis. «The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for». *Computer Law & Security Review*, vol. 25, n.º 1 (2009), p. 403-414.

De Hert Paul y Bellanova, Rocco. «Data protection in the Area of Freedom, Security and Justice. A system still to be fully developed?». *Briefing Paper.* European Parliament, Directorate General Internal Policies of the Union, Policy Department C, Citizens' Rights and Constitutional Affairs. PE 410.692 (marzo de 2009), p. 23.

Hayes, Ben. «From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained». *Statewatch Analysis* (2004).

Hayes, Ben y Vermeulen, Mathias. *Borderline. The EU's new border surveillance initiatives: Assessing the costs and fundamental rights implications of EUROSUR and the "Smart Borders" proposals*. Berlín: Heinrich Böll Foundation, 2012, p. 82.

Hijmans Hielke y Scirocco Alfonso. «Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?». *Common Market Law Review*, vol. 46, n.º 5 (2009), p. 1.485-1.525.

Parlamento Europeo. *Resolución del Parlamento Europeo, de 22 de mayo de 2012, sobre la Estrategia de Seguridad Interior de la Unión Europea* ((2010)2308 (INI)).

Peers, Steve. «Analysis. The Directive on data protection and law enforcement: A Missed Opportunity?». *Statewatch* (abril de 2012), p. 5.

SEPD-Supervisor Europeo de Protección de Datos. «Opinión sobre el paquete de reforma de protección de datos» (7.03.2012a).

SEPD-Supervisor Europeo de Protección de Datos. «Opinión sobre Eurodac» (5.09.2012b).

Statewatch. «Law enforcement authorities to gain access to European visa database on 1 September». *Statewatch*, n.º 32500 (3.07.2013). http://database.statewatch.org/article.asp?aid=32500

Statewatch. «Schengen Information System: 41,000 people subject to discreet surveillance or specific checks». *News* (9 de septiembre de 2014) (en línea) [Fecha de consulta: 12.05.2015] http://www.statewatch.org/news/2014/sep/sis-stats.htm

Steria. «European Commission deploys Visa Information System developed by Steria-led consortium». *STERIA Press Release* (10 de septiembre de 2012) (en línea) [Fecha de consulta: 12.05.2015] http://www.steria.com/sg/media/press-releases/press-releases/article/european-commission-deploys-visa-information-system-developed-by-steria-led-consortium/

TJUE-Tribunal de Justicia de la UE. *C-293/12 y C-594/12*. «Digital Rights Ireland Ltd, Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl y otros c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Irlanda y el Attorney General» (16 de mayo de 2014).

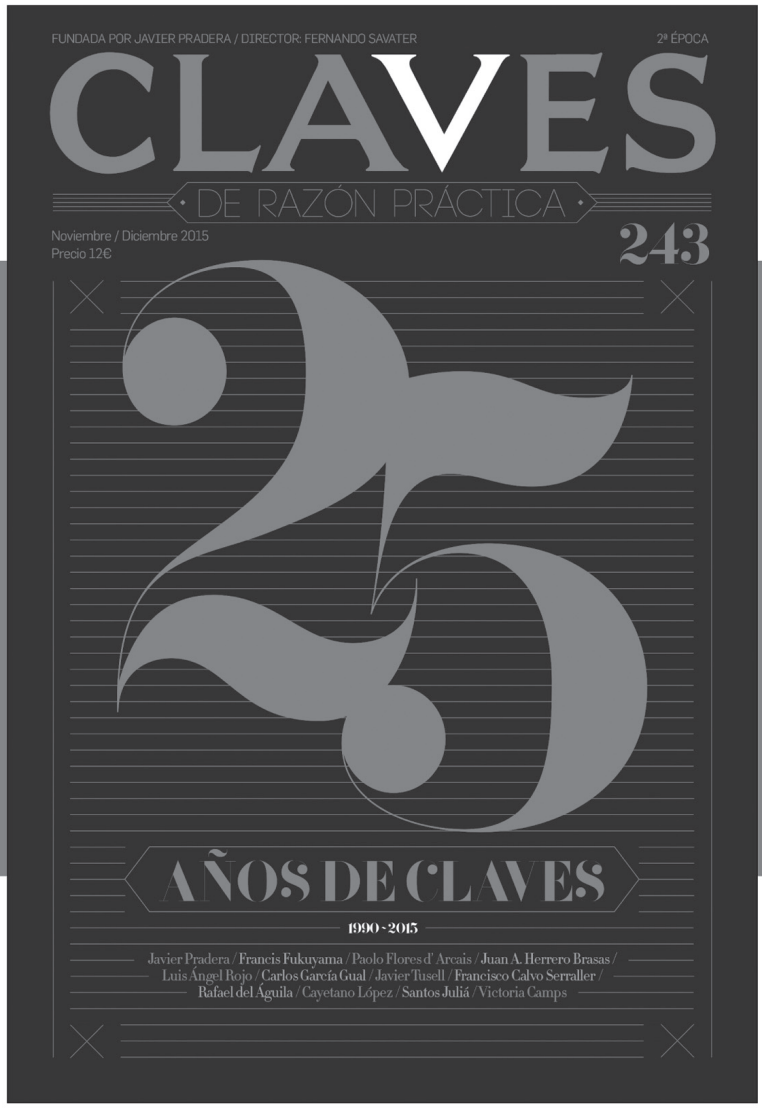
Unión Europea. «Reglamento (UE) n.° 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los estados miembros por un nacional de un tercer país o un apátrida». DO L 80 (29.06.2013), p. 1-30.

NÚMERO ESPECIAL ANIVERSARIO

25 AÑOS DE CLAVES

CON UNA SELECCIÓN DE ARTÍCULOS DE

Javier Pradera / Francis Fukuyama / Paolo Flores d' Arcais / Juan A. Herrero Brasas / Luis Ángel Rojo / Carlos García Gual / Javier Tusell / Francisco Calvo Serraller / Rafael del Águila / Cayetano López / Santos Juliá / Victoria Camps



Dirigida por Fernando Savater.

Suscripciones: 902 101 146 **prisarevistas.com/claves**

Disponible en: K+ KIOSKO Y MÁS